Abstract

The invention provides a method for encrypting a program for execution on a remote host computer on a network, such that correct execution by the remote host computer is ensured, and such that the remote host computer remains unaware of the computations or data associated with execution. Results from the computations at the remote host computer are transmitted to a control computer, on the network, which decodes the results to useful data representative as output from the program. In a first step of the method, the program is encoded as a unitary matrix multiplication, U_{ij}, of i dimensions by j dimensions. U_n is the set of unitary matrices of size n, forms a non-commutatitive group under matrix multiplication, and has a unique group-invariant Haar measure probability distribution; U_{ij} is thus an element of U_n. In a second step, an input data string to the program is encoded as a vector b_j of n dimensions. The first and second steps can be performed in either order. In a third step, two independent identically distributed unitary matrices X_{ij}, Y_{ij} are generated from the Haar distribution over U_n. Preferably, X_{ij}, Y_{ij} are randomly generated. In a fourth step, U' is computed as XUY* and sent to the remote host over the network. In a fifth step, b' is computed as Yb and sent to the remote host over the network. The fourth and fifth steps can be performed in either order. In a sixth step, the remote host computes the product of XUY* and Yb and sends the result to the control computer on the network. In a seventh step, the control computer computes X*XUb to determine the multiplication of Ub, the desired output of the program.